

SYSTEM AND METHOD FOR ANALYZING ILLEGAL ACCESS ROUTE

Publication number: JP2003258910 (A)

Publication date: 2003-09-12

Also published as:

JP3892322 (B2)

Inventor(s): KITAZAWA SHIGEKI +

Applicant(s): MITSUBISHI ELECTRIC CORP +

Classification:

- international: G06F13/00; G06F15/00; H04L12/22; H04L12/56; G06F13/00;
G06F15/00; H04L12/22; H04L12/56; (IPC1-7): G06F13/00;
G06F15/00; H04L12/22; H04L12/56

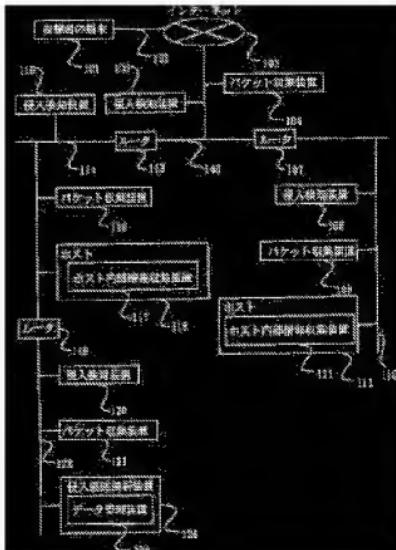
- European:

Application number: JP20020056913 20020304

Priority number(s): JP20020056913 20020304

Abstract of JP 2003258910 (A)

PROBLEM TO BE SOLVED: To realize intrusion route analysis which is applicable to intrusion using a steppingstone and intrusion using a false transmission-source address. **SOLUTION:** A packet gathering device 104, etc., records the header contents of a packet sent through a network as header information and a host internal information gathering device 111, etc., gathers internal process information regarding internal processes of a host 112, etc. An intrusion route analyzing device 124 receives the header information and internal process information and a data management device 123 manages data as a database; ; when an intrusion packet is detected, the transmission source of the intrusion packet is detected by using host level analysis and router level analysis in combination and when the transmission source of the intrusion packet is a host in the network, a packet which contributes the generation and transmission of the intrusion packet is specified by taking host internal analysis of the host to analyze the intrusion route by using the three analyzing processes in combination. ; **COPYRIGHT:** (C) 2003,JPO



Data supplied from the **espacenet** database — Worldwide

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-258910

(P2003-258910A)

(43)公開日 平成15年9月12日(2003.9.12)

(51)IntCL⁷
 H 0 4 L 12/56
 G 0 6 F 13/00
 15/00
 H 0 4 L 12/22

識別記号
 4 0 0
 3 5 1
 3 2 0
 H 0 4 L 12/22

F I
 H 0 4 L 12/56
 G 0 6 F 13/00
 15/00
 H 0 4 L 12/22

5-73-1*(参考)
 4 0 0 Z 5 B 0 8 5
 3 5 1 Z 5 B 0 8 9
 3 2 0 A 5 K 0 3 0

審査請求 未請求 請求項の数16 O.L (全 16 頁)

(21)出願番号 特願2002-56913(P2002-56913)
 (22)出願日 平成14年3月4日(2002.3.4)

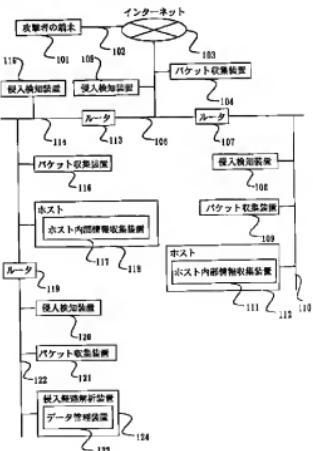
(71)出願人 000006013
 三菱電機株式会社
 東京都千代田区丸の内二丁目2番3号
 (72)発明者 北澤 繁樹
 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内
 (74)代理人 100099461
 弁理士 溝井 章司 (外5名)
 Fターム(参考) 5B085 AC11
 5B089 GB02 KA17 KB13
 5K030 GA15 HA08 JA10 KA05 KX24
 KX90 LC14 LC15 LD19

(54)【発明の名称】 不正アクセス経路解析システム及び不正アクセス経路解析方法

(57)【要約】

【課題】 踏み台を用いた侵入、発信元アドレスを詐称した侵入に対しても対応可能な侵入経路解析を実現する。

【解決手段】 パケット収集装置104等がネットワーク上を流れるパケットのヘッダ内容をヘッダ情報として記録し、ホスト内部情報収集装置111等がホスト112等の内部プロセスに関する内部プロセス情報を収集し、侵入経路解析装置124はヘッダ情報及び内部プロセス情報を受信するとともにデータ管理装置123においてデータベースとして管理し、侵入パケットの検知の際に、ホストレベル解析及びルータレベル解析を併用して侵入パケットの送信元を検出し、侵入パケットの送信元がネットワーク内のホストであった場合には、当該ホストに対してホスト内部解析を行って侵入パケットの生成・送信に関与したパケットを特定し、以後、3つの解析処理を併用して侵入経路の解析を行う。



【特許請求の範囲】

【請求項1】 相互にパケット送受信を行い得る複数のデータ処理装置を含む所定のネットワークを管理対象とし、前記ネットワークに含まれるいずれかのデータ処理装置に対して不正アクセスパケットが送信された場合に、不正アクセスパケットの送信に用いられた不正アクセス経路の解析を行う不正アクセス経路解析システムであって、

前記ネットワークを流通するパケットを監視し、不正アクセスパケットを検知するパケット監視部と、前記パケット監視部により不正アクセスパケットが検知された場合に、不正アクセスパケットの送信元の検出処理を行い、所定の場合に、前記複数のデータ処理装置のうち特定のデータ処理装置を不正アクセスパケットの送信元として検出する送信元検出処理部と、前記送信元検出処理部により特定のデータ処理装置が不正アクセスパケットの送信元として検出された場合に、前記送信元検出処理部により検出されたデータ処理装置の内部プロセスについて解析処理を行って、不正アクセスパケットの生成及び送信を実行した内部プロセスを不正アクセスパケット生成送信プロセスとして検出するとともに、所定の場合に、前記不正アクセスパケット生成送信プロセスに関連するパケット受信プロセスを検出し、検出した前記パケット受信プロセスにおいて受信されたパケットを不正アクセスパケットとして認定する内部プロセス解析処理部とを有し、

前記送信元検出処理部は、

前記内部プロセス解析処理部により不正アクセスパケットの認定が行われた場合に、認定された不正アクセスパケットの送信元の検出処理を行うことを特徴とする不正アクセス経路解析システム。

【請求項2】 前記不正アクセス経路解析システムは、更に、前記複数のデータ処理装置の各々の内部プロセスを監視し、所定の場合に、前記内部プロセス解析処理部に特定のデータ処理装置に関する通知を行う内部プロセス監視部を有し、

前記内部プロセス解析処理部は、

前記内部プロセス監視部から通知されたデータ処理装置の内部プロセスについて解析処理を行い、不正アクセスパケット生成送信プロセスに関連するパケット受信プロセスが検出された場合に、不正アクセスパケットの認定を行い、

前記送信元検出処理部は、

前記内部プロセス解析処理部により不正アクセスパケットの認定が行われた場合に、認定された不正アクセスパケットの送信元の検出処理を行うことを特徴とする請求項1に記載の不正アクセス経路解析システム。

【請求項3】 前記送信元検出処理部及び前記内部プロセス解析処理部は、相互に連動してそれぞれの処理を行

い、

前記送信元検出処理部は、

前記内部プロセス解析処理部により不正アクセスパケットの認定が行われる度に、認定された不正アクセスパケットの送信元の検出処理を行い、所定の場合に、特定のデータ処理装置を不正アクセスパケットの送信元として検出し、

前記内部プロセス解析処理部は、

前記送信元検出処理部により特定のデータ処理装置が不正アクセスパケットの送信元として検出される度に、前記送信元検出処理部により検出されたデータ処理装置の内部プロセスについて解析処理を行い、不正アクセスパケット生成送信プロセスに関連するパケット受信プロセスが検出された場合に、不正アクセスパケットの認定を行うことを特徴とする請求項1又は2に記載の不正アクセス経路解析システム。

【請求項4】 前記内部プロセス解析処理部は、特定のデータ処理装置の内部プロセスについて解析処理を行った結果、不正アクセスパケット生成送信プロセスに関連するパケット受信プロセスが検出されなかった場合に、前記特定のデータ処理装置を不正アクセスの始点と判断することを特徴とする請求項1～3のいずれかに記載の不正アクセス経路解析システム。

【請求項5】 前記不正アクセス経路解析システムは、データ処理装置間に少なくなくとも一つ以上のパケット中継装置が配置されたネットワークを管理対象とし、前記送信元検出処理部は、不正アクセスパケットを受信したデータ処理装置を始点として、不正アクセスパケットを中継したパケット中継装置を論理的に順次辿って不正アクセスパケットの送信元を検出する第一の送信元検出処理と、不正アクセスパケットに含まれた送信元を示す送信元アドレス情報に基づき、不正アクセスパケットの送信元を検出する第二の送信元検出処理とを並行して行うことを行つことを特徴とする請求項1～3のいずれかに記載の不正アクセス経路解析システム。

【請求項6】 前記第二の送信元検出処理は前記第一の送信元検出処理よりも早期に完了する場合があり、前記内部プロセス解析処理部は、

前記第二の送信元検出処理が前記第一の送信元検出処理よりも早期に完了し、不正アクセスパケットの送信元として特定のデータ処理装置が検出された場合に、前記第二の送信元検出処理により検出されたデータ処理装置の内部プロセスについて解析処理を行い、

前記第二の送信元検出処理により検出されたデータ処理装置の内部プロセスについての解析処理の実行中に、前記第一の送信元検出処理が完了し前記第二の送信元検出処理とは異なるデータ処理装置が不正アクセスパケットの送信元として検出された場合に、前記第二の送信元検出処理により検出されたデータ処理装置の内部プロセス

についての解析処理を終了し、前記第一の送信元検出処理により検出されたデータ処理装置の内部プロセスについての解析処理を開始することを特徴とする請求項5に記載の不正アクセス経路解析システム。

【請求項7】 前記不正アクセス経路解析システムは、更に、

前記ネットワーク内の少なくとも一以上の箇所で前記ネットワークを流通する複数のパケットを収集し、収集した複数のパケットのヘッダの内容を複数のヘッダ情報をとして記録し、記録した複数のヘッダ情報を前記送信元検出処理部に送信するパケット收集部を有し、

前記送信元検出処理部は、

前記パケット收集部より前記複数のヘッダ情報を受信するとともに、前記第一の送信元検出処理として、

データ処理装置が受信した不正アクセスパケットのヘッダに含まれる情報であって送信元Etherアドレス、宛先Etherアドレス及びTTL(TimeToLive)値以外の情報に基づき、前記複数のヘッダ情報の中から少なくとも一つ以上のヘッダ情報を抽出ヘッダ情報として抽出し、不正アクセスパケットに含まれる送信元Etherアドレス、宛先Etherアドレス及びTTL値を始点として抽出ヘッダ情報に含まれる送信元Etherアドレス、宛先Etherアドレス及びTTL値の更新経過を順次遡って不正アクセスパケットの送信元を検出することを特徴とする請求項5に記載の不正アクセス経路解析システム。

【請求項8】 前記送信元検出処理部は、

前記第二の送信元検出処理として、

不正アクセスパケットに含まれた送信元IPアドレスに基づき、不正アクセスパケットの送信元を検出することを特徴とする請求項5に記載の不正アクセス経路解析システム。

【請求項9】 前記パケット收集部は、

前記送信元検出処理部から指示があった場合のみ、パケットの収集を行うことを特徴とする請求項7に記載の不正アクセス経路解析システム。

【請求項10】 前記パケット收集部は、

前記送信元検出処理部から指示があった場合のみ、前記送信元検出処理部に対して前記複数のヘッダ情報を送信することを特徴とする請求項7に記載の不正アクセス経路解析システム。

【請求項11】 前記不正アクセス経路解析システムは、更に、

前記複数のデータ処理装置の各々について内部プロセスに関する情報を内部プロセス情報として収集し、収集した内部プロセス情報を前記内部プロセス解析処理部へ送信する内部プロセス情報收集部を有し、

前記内部プロセス解析処理部は、

前記内部プロセス情報收集部より前記内部プロセス情報

を受信するとともに、受信した内部プロセス情報の中から内部プロセス解析処理の対象となるデータ処理装置の内部プロセス情報を選択し、選択した内部プロセス情報を用いて内部プロセス解析処理を行うことを特徴とする請求項1～3のいずれかに記載の不正アクセス経路解析システム。

【請求項12】 前記内部プロセス情報收集部は、前記内部プロセス解析処理部から指示があった場合のみ、内部プロセス情報の収集を行うことを特徴とする請求項11に記載の不正アクセス経路解析システム。

【請求項13】 前記内部プロセス情報收集部は、前記内部プロセス解析処理部から指示があつた場合のみ、前記内部プロセス解析処理部に対して前記内部プロセス情報を送信することを特徴とする請求項11に記載の不正アクセス経路解析システム。

【請求項14】 前記不正アクセス経路解析システムは、他のネットワークを管理対象とする他の不正アクセス経路解析システムと通信可能であり、

前記他の不正アクセス経路解析システムより、前記他のネットワーク内で検出された他ネットワーク不正アクセスパケットの情報を含む検出依頼を受信した場合に、前記送信元検出処理部は、

前記検出依頼に含まれた前記他ネットワーク不正アクセスパケットの情報に基づき、前記他ネットワーク不正アクセスパケットの送信元の検出処理を行ふことを特徴とする請求項1に記載の不正アクセス経路解析システム。

【請求項15】 前記不正アクセス経路解析システムは、他のネットワークを管理対象とする他の不正アクセス経路解析システムと通信可能であり、

前記送信元検出処理部が特定の不正アクセスパケットについて送信元が検出できなかった場合に、前記他の不正アクセス経路解析システムに対して前記特定の不正アクセスパケットの送信元の検出を依頼する検出依頼を送信することを特徴とする請求項1に記載の不正アクセス経路解析システム。

【請求項16】 相互にパケット送受信を行い得る複数のデータ処理装置を含む所定のネットワークを管理対象とし、前記ネットワークに含まれるいずれかのデータ処理装置に対して不正アクセスパケットが送信された場合に、不正アクセスパケットの送信元に用いられた不正アクセス経路の解析を行う不正アクセス経路解析方法であつて、

前記ネットワークを流通するパケットを監視し、不正アクセスパケットを検知するパケット監視ステップと、前記パケット監視ステップにより不正アクセスパケットが検知された場合に、不正アクセスパケットの送信元の検出処理を行い、所定の場合に、前記複数のデータ処理装置のうち特定のデータ処理装置を不正アクセスパケットの送信元として検出する送信元検出処理ステップと、前記送信元検出処理ステップにより特定のデータ処理装

置が不正アクセスパケットの送信元として検出された場合に、前記送信元検出処理ステップにより検出されたデータ処理装置の内部プロセスについて解析処理を行って、不正アクセスパケットの生成及び送信を実行した内部プロセスを不正アクセスパケット生成送信プロセスとして検出するとともに、所定の場合に、前記不正アクセスパケット生成送信プロセスに関するパケット受信プロセスを検出し、検出した前記パケット受信プロセスにおいて受信されたパケットを不正アクセスパケットとして認定する内部プロセス解析処理ステップとを有し、前記送信元検出処理ステップは、

前記内部プロセス解析処理ステップにより不正アクセスパケットの認定が行われた場合に、認定された不正アクセスパケットの送信元の検出処理を行うことを特徴とする不正アクセス経路解析方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、侵入経路解析システム並びに、侵入経路解析手法の高速化に関するものである。

【0002】

【從来の技術】図2は例えば、特開2000-341315および特開2000-124952に示されたパケットの情報を解析する從来の侵入経路解析システムを示す。図2において、201は攻撃者端末、202はインターネット、203は攻撃者端末が直接接続しているアクセスサーバ、206は踏み台ホスト、211は不正アクセス対象ホスト、210は侵入検知装置、204、205は攻撃者端末201から踏み台ホスト206へのパケットを中継した追跡装置（ルータ）、207、208、209は踏み台ホストから不正アクセス対象ホストへのパケットを中継した追跡装置（ルータ）である。攻撃者は、踏み台ホスト206を使用することで不正アクセス対象ホスト211に対して攻撃者端末の身元を隠蔽して不正アクセスを行っているものとする。

【0003】このような從来の侵入追跡システムにおいては、不正アクセス対象ホスト211から踏み台ホスト206までの追跡と踏み台ホスト206から攻撃者端末201までの追跡処理が複数の段階を経る。どの段階においても不正アクセスパケットの情報を元に追跡管理装置212が追跡経路上に存在する複数の追跡装置（ルータ）へ追跡を指示し、その結果からさらにその先の追跡装置（ルータ）へ追跡を指示するといった逐次的な追跡を継続することで攻撃者端末201が直接接続しているアクセスサーバ203まで追跡を行う。最終的な攻撃者端末201の特定はアクセスサーバ203の接続ログを解析することである。

【0004】図3は例えば、特開平10-164064に示された接続経路情報をホスト間の接続ごと、あらかじめ記録として残しておく從来の侵入経路解析システム

である。図3において、301はネットワーク管理マネージャ、302、303、304は計算機ノード、305は追跡情報収集操作、306はセキュリティ上の問題通知を表している。図において、計算機ノード302から計算機ノード303を踏み台として、計算機ノード304へ不正なアクセスを行っているものとする。また、各計算機ノードは、リモートから接続が行われたとき、その接続の経路追跡を行うための情報をあらかじめ記録しておく。

【0005】このような從来の侵入追跡システムにおいては、図3の計算機ノード303から計算機ノード304へ接続を要求した場合、計算機ノード304は、経路追跡に使用する接続経路情報を計算機ノード303へ要求する。計算機ノード303は、接続を要求している計算機ノード303上のプロセスの識別子と計算機ノード303の識別子を計算機ノード304へ送る。同様の手続きは、計算機ノード間の接続が発生するたびに行われているものとする。セキュリティ上の問題が計算機ノード304上で起こったとき、ネットワーク管理マネージャ301は計算機ノード304からのセキュリティ上の問題通知306を受け取り、計算機ノード304上に記録されている、そのセキュリティ上の問題が発生させる元となった接続経路情報を元に、計算機ノード303へ計算機ノード304との接続経路情報を問い合わせる。計算機ノード303では、計算機ノード304への接続は計算機ノード302からの接続により起動されたプロセスにより発生していることをネットワーク管理マネージャ301へ通知する。次にネットワーク管理マネージャ301は、計算機ノード302へ接続経路情報の問い合わせを行い、最終的に計算機ノード302が不正なアクセスを行った接続経路の発信源であると特定する。

【0006】

【発明が解決しようとする課題】従来の侵入経路解析システムのうち、特開2000-341315及び特開2000-124952に示されたものは、パケットのヘッダ情報を元に侵入経路を解析することでIPパケットのヘッダ情報に含まれている発信元アドレスを詐称した不正アクセスパケットの追跡が可能という利点がある反面、踏み台を介した攻撃については、踏み台ホストの入出力を監視し、不正アクセスパケットが再び踏み台ホストへ送信されるのを待つ必要があり、侵入経路追跡の継続性を積極的に維持できない、追跡時間がかかるなどの問題点があった。一方、接続経路情報をホスト間の接続ごとにあらかじめ記録として残しておく方式（特開平10-164064）では、侵入経路追跡にかかる時間を短縮できる代わりに、IPパケットのヘッダ情報に含まれている発信元アドレスを詐称した攻撃では、偽の接続経路情報が記録されることもありうるため、正確性に問題点があった。また、いずれの場合にも追跡処理を管理するホストが侵入経路上のルータもしくは、接続ホスト

一つ一つと通信を行なながら逐次追跡していくため、侵入経路上のルータおよびホストの数に比例して侵入経路解析時間が増加する問題点があった。

【0007】この発明は上記のような問題点を解決するためになされたもので、攻撃者が身元を隠蔽する行為（例えば発信元IPアドレスの偽称、踏み台ホストの使用など）を行った場合であっても侵入経路解析結果を正確かつ高速に求めができる侵入経路解析システムのためのシステム構成と解析アルゴリズムに関するものである。

【0008】

【課題を解決するための手段】本発明に係る不正アクセス経路解析システムは、相互にパケット送受信を行なう複数のデータ処理装置を含む所定のネットワークを管理対象とし、前記ネットワークに含まれるいづれかのデータ処理装置に対して不正アクセスパケットが送信された場合に、不正アクセスパケットの送信に用いられた不正アクセス経路の解析を行う不正アクセス経路解析システムであって、前記ネットワークを通過するパケットを監視し、不正アクセスパケットを検知するパケット監視部と、前記パケット監視部により不正アクセスパケットが検知された場合に、不正アクセスパケットの送信元の検出処理を行い、所定の場合に、前記複数のデータ処理装置のうち特定のデータ処理装置を不正アクセスパケットの送信元として検出する送信元検出処理部と、前記送信元検出処理部により特定のデータ処理装置が不正アクセスパケットの送信元として検出された場合に、前記送信元検出処理部により検出されたデータ処理装置の内部プロセスについて解析処理を行って、不正アクセスパケットの生成及び送信を実行した内部プロセスを不正アクセスパケット生成送信プロセスとして検出するとともに、所定の場合に、前記不正アクセスパケット生成送信プロセスに連携するパケット受信プロセスを検出し、検出した前記パケット受信プロセスにおいて受信されたパケットを不正アクセスパケットとして認定する内部プロセス解析処理部とを有し、前記送信元検出処理部は、前記内部プロセス解析処理部により不正アクセスパケットの認定が行われた場合に、認定された不正アクセスパケットの送信元の検出処理を行なうことを特徴とする。

【0009】前記不正アクセス経路解析システムは、更に、前記複数のデータ処理装置の各々の内部プロセスを監視し、所定の場合に、前記内部プロセス解析処理部に特定のデータ処理装置に関する通知を行なう内部プロセス監視部を有し、前記内部プロセス解析処理部は、前記内部プロセス監視部から通知されたデータ処理装置の内部プロセスについて解析処理を行い、不正アクセスパケット生成送信プロセスに連携するパケット受信プロセスが検出された場合に、不正アクセスパケットの認定を行い、前記送信元検出処理部は、前記内部プロセス解析処理部により不正アクセスパケットの認定が行われた場合

に、認定された不正アクセスパケットの送信元の検出処理を行なうことを特徴とする。

【0010】前記送信元検出処理部及び前記内部プロセス解析処理部は、相互に連動してそれぞれの処理を行い、前記送信元検出処理部は、前記内部プロセス解析処理部により不正アクセスパケットの認定が行われる度に、認定された不正アクセスパケットの送信元の検出処理を行なう場合に、特定のデータ処理装置を不正アクセスパケットの送信元として検出し、前記内部プロセス解析処理部は、前記送信元検出処理部により特定のデータ処理装置が不正アクセスパケットの送信元として検出される度に、前記送信元検出処理部により検出されたデータ処理装置の内部プロセスについて解析処理を行なう、不正アクセスパケット生成送信プロセスに連携するパケット受信プロセスが検出された場合に、不正アクセスパケットの認定を行なうことを特徴とする。

【0011】前記内部プロセス解析処理部は、特定のデータ処理装置の内部プロセスについて解析処理を行なった結果、不正アクセスパケット生成送信プロセスに連携するパケット受信プロセスが検出されなかった場合に、前記特定のデータ処理装置を不正アクセスの始点と判断することを特徴とする。

【0012】前記不正アクセス経路解析システムは、データ処理装置間に少なくなくとも一つ以上のパケット中継装置が配置されたネットワークを管理対象とし、前記送信元検出処理部は、不正アクセスパケットを受信したデータ処理装置を始点として、不正アクセスパケットを中継したパケット中継装置を論理的に順次順て不正アクセスパケットの送信元を検出する第一の送信元検出処理と、不正アクセスパケットに含まれた送信元を示す送信元アドレス情報を基づき、不正アクセスパケットの送信元を検出する第二の送信元検出処理とを並行して行なうことを特徴とする。

【0013】前記第二の送信元検出処理は前記第一の送信元検出処理よりも早期に完了する場合があり、前記内部プロセス解析処理部は、前記第二の送信元検出処理が前記第一の送信元検出処理よりも早期に完了し、不正アクセスパケットの送信元として特定のデータ処理装置が検出された場合に、前記第二の送信元検出処理により検出されたデータ処理装置の内部プロセスについて解析処理を行い、前記第二の送信元検出処理により検出されたデータ処理装置の内部プロセスについての解析処理の実行中に、前記第一の送信元検出処理が完了し前記第二の送信元検出処理とは異なるデータ処理装置が不正アクセスパケットの送信元として検出された場合に、前記第二の送信元検出処理により検出されたデータ処理装置の内部プロセスについての解析処理を終了し、前記第一の送信元検出処理により検出されたデータ処理装置の内部プロセスについての解析処理を開始することを特徴とする。

【0014】前記不正アクセス経路解析システムは、更に、前記ネットワーク内の少なくとも一以上の箇所で前記ネットワークを流れる複数のパケットを収集し、収集した複数のパケットのヘッダの内容を複数のヘッダ情報として記録し、記録した複数のヘッダ情報を前記送信元検出処理部に送信するパケット收集部を有し、前記送信元検出処理部は、前記パケット收集部よりも前記複数のヘッダ情報を受信するとともに、前記第一の送信元検出処理として、データ処理装置が受信した不正アクセスパケットのヘッダに含まれる情報であって送信元Etherアドレス、宛先Etherアドレス及びTTL(Time To Live)値以外の情報に基づき、前記複数のヘッダ情報の中から少なくとも一つ以上のヘッダ情報を抽出ヘッダ情報として抽出し、不正アクセスパケットに含まれる送信元Etherアドレス、宛先Etherアドレス及びTTL値を始点として抽出ヘッダ情報を含まれる送信元Etherアドレス、宛先Etherアドレス及びTTL値の更新経過を順次通過して不正アクセスパケットの送信元を検出することを特徴とする。

【0015】前記送信元検出処理部は、前記第二の送信元検出処理として、不正アクセスパケットに含まれた送信元IPアドレスに基づき、不正アクセスパケットの送信元を検出することを特徴とする。

【0016】前記パケット收集部は、前記送信元検出処理部から指示があった場合のみ、パケットの收集を行うことを特徴とする。

【0017】前記パケット收集部は、前記送信元検出処理部から指示があった場合のみ、前記送信元検出処理部に対して前記複数のヘッダ情報を送信することを特徴とする。

【0018】前記不正アクセス経路解析システムは、更に、前記複数のデータ処理装置の各々について内部プロセスに関する情報を内部プロセス情報として収集し、収集した内部プロセス情報を前記内部プロセス解析処理部へ送信する内部プロセス情報收集部を有し、前記内部プロセス解析処理部は、前記内部プロセス情報收集部より前記内部プロセス情報を受信するとともに、受信した内部プロセス情報を中から内部プロセス解析処理の対象となるデータ処理装置の内部プロセス情報を選択し、選択した内部プロセス情報を用いて内部プロセス解析処理を行うことを特徴とする。

【0019】前記内部プロセス情報收集部は、前記内部プロセス解析処理部から指示があった場合のみ、内部プロセス情報の收集を行うことを特徴とする。

【0020】前記内部プロセス情報收集部は、前記内部プロセス解析処理部から指示があった場合のみ、前記内部プロセス解析処理部に対して前記内部プロセス情報を送信することを特徴とする。

【0021】前記不正アクセス経路解析システムは、他のネットワークを管理対象とする他の不正アクセス経路

解析システムと通信可能であり、前記他の不正アクセス経路解析システムより、前記他のネットワーク内で検出された他ネットワーク不正アクセスパケットの情報を含む検出依頼を受信した場合に、前記送信元検出処理部は、前記検出依頼に含まれた前記他ネットワーク不正アクセスパケットの情報に基づき、前記他ネットワーク不正アクセスパケットの送信元の検出処理を行うことを特徴とする。

【0022】前記不正アクセス経路解析システムは、他のネットワークを管理対象とする他の不正アクセス経路解析システムと通信可能であり、前記送信元検出処理部が特定の不正アクセスパケットについて送信元が検出できなかった場合に、前記他の不正アクセス経路解析システムに対して前記特定の不正アクセスパケットの送信元の検出を依頼する検出依頼を送信することを特徴とする。

【0023】本発明に係る不正アクセス経路解析方法は、相互にパケット送受信を行い得る複数のデータ処理装置を含む所定のネットワークを管理対象とし、前記ネットワークに含まれるいずれかのデータ処理装置に対して不正アクセスパケットが送信された場合に、不正アクセスパケットの送信に用いられた不正アクセス経路の解析を行なう不正アクセス経路解析方法であって、前記ネットワークを流通するパケットを監視し、不正アクセスパケットを検知するパケット監視ステップと、前記パケット監視ステップにより不正アクセスパケットが検知された場合に、不正アクセスパケットの送信元の検出処理を行い、所定の場合に、前記複数のデータ処理装置のうち特定のデータ処理装置を不正アクセスパケットの送信元

として検出する送信元検出処理ステップと、前記送信元検出処理ステップにより特定のデータ処理装置が不正アクセスパケットの送信元として検出された場合に、前記送信元検出処理ステップにより検出されたデータ処理装置の内部プロセスについて解析処理を行って、不正アクセスパケットの生成及び送信を実行した内部プロセスを不正アクセスパケット生成送信プロセスとして検出するとともに、所定の場合に、前記不正アクセスパケット生成送信プロセスに隣接するパケット受信プロセスを検出し、検出した前記パケット受信プロセスにおいて受信されたパケットを不正アクセスパケットとして認定する内部プロセス解析処理ステップとを有し、前記送信元検出処理ステップは、前記内部プロセス解析処理ステップにより不正アクセスパケットの認定が行われた場合に、認定された不正アクセスパケットの送信元の検出処理を行うことを特徴とする。

【0024】
【発明の実施の形態】実施の形態1. 図1は侵入経路解析システム(不正アクセス経路解析システム)の全体図を表す構成図である。ただし、図1はこの侵入経路解析

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
559
560
561
562
563
564
565
566
567
568
569
569
570
571
572
573
574
575
576
577
578
579
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
618
619
619
620
621
622
623
624
625
626
627
628
629
629
630
631
632
633
634
635
636
637
638
639
639
640
641
642
643
644
645
646
647
648
649
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
688
689
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
718
719
719
720
721
722
723
724
725
726
727
728
729
729
730
731
732
733
734
735
736
737
738
739
739
740
741
742
743
744
745
746
747
748
749
749
750
751
752
753
754
755
756
757
758
759
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
776
777
778
779
779
780
781
782
783
784
785
786
787
788
789
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
818
819
819
820
821
822
823
824
825
826
827
828
829
829
830
831
832
833
834
835
836
837
838
839
839
840
841
842
843
844
845
846
847
848
849
849
850
851
852
853
854
855
856
857
858
859
859
860
861
862
863
864
865
866
867
868
869
869
870
871
872
873
874
875
876
877
878
879
879
880
881
882
883
884
885
886
887
888
889
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
909
910
911
912
913
914
915
916
917
918
919
919
920
921
922
923
924
925
926
927
928
929
929
930
931
932
933
934
935
936
937
938
939
939
940
941
942
943
944
945
946
947
948
949
949
950
951
952
953
954
955
956
957
958
959
959
960
961
962
963
964
965
966
967
968
969
969
970
971
972
973
974
975
976
977
978
979
979
980
981
982
983
984
985
986
987
988
989
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2099
2100

析スケジューリングをそれぞれの解析時系列（414、415、416）上に表したものである。図4において、解析時系列（414、415、416）上の長方形は、その解析が実行中であることを示している。図4において、414はホストレベル解析を、415はホスト内部解析を、416はルータレベル解析を示している。

【0029】ホストレベル解析は、侵入検知装置により検知された侵入パケットに含まれた送信元IPアドレスに基づき、侵入パケットの送信元を検出する解析手法である。また、パケットがたとえばRFC(Request for Comments)で規定されるような通信プロトコルに違反していないかどうかの解析も行う。また、パケットのヘッダ情報に含まれる発信元IPアドレスが実際にネットワークへ接続可能なIPアドレスであるかどうかなどの調査(DNSの参照やパケット到達性の検査)もあわせて行う。したがって、一般的には短時間で解析処理が終了する反面、IPアドレスを偽称された場合に対応できないため、解析結果の正確性に乏しい。なお、ホストレベル解析は、第二の送信元検出処理に相当する。一方、ルータレベル解析は、パケット収集装置より送信されたヘッダ情報のうち送信元Etherアドレス、宛先Etherアドレス、TTLに基づいて、侵入パケットを中継したルータを論理的に順次週って侵入パケットの送信元を検出する解析手法である。ルータレベル解析は、パケットのIPアドレスによらず解析を行うので、IPアドレスを偽称された場合でも正確にパケットの送出ホストと中継経路を特定できる反面、一般的には解析に時間がかかる。なお、ルータレベル解析の具体的手順については後述する。また、ルータレベル解析は、第一の送信元検出処理に相当する。ホスト内部解析は、ホストレベル解析、ルータレベル解析によりホストが特定された場合、またはホスト内部を監視する侵入検知装置によりホストが特定された場合に、特定されたホストの内部プロセス状況を解析し、そのホストが侵入パケットの生成及び送信を行ったか否かを判断するとともに、そのホストが受信したパケットのうち侵入パケットの生成及び送信に関与したパケットを特定する解析手法である。ホスト内部解析の具体的手順についても後述する。

【0030】図1の侵入経路解析装置124は以下の解析の開始および終了の条件に従って侵入経路解析を継続もしくは終了する。ネットワークを流れるパケットを監視している侵入検知装置から侵入検知通知があった場合には、まず、ホストレベル解析とルータレベル解析を平行して実行する(401、409)。また、ホストの内部状態を監視する侵入検知装置から侵入検知通知があった場合には、まず、ホスト内部解析を実行する。ホストレベル解析終了時(402、403、404)、そのホストレベル解析と同時に開始されたルータレベル解析(たとえば、401で開始されたホストレベル解析)に対

する409で開始されたルータレベル解析)が未終了か否、ホストレベル解析の結果により、ホスト内部解析の対象となるホストが侵入経路解析装置の管理下に存在する場合に、ホストレベル解析の入力としたパケットの情報を元にホスト内部解析を開始する(402、404)。その他の場合はホスト内部解析を開始しない(403)。ルータレベル解析終了時(410、411、412)、そのルータレベル解析と同時に開始されたホストレベル解析(たとえば、409で開始されたルータレベル解析に対する401で開始されたホストレベル解析)が未終了または、ルータレベル解析結果を得られたパケット生成ホストの発信元Etherアドレスを持つホストのアドレスとルータレベル解析の検索キーとしたパケットの発信元アドレスが異なる場合並びに、ホスト内部解析の対象となるホストが侵入経路解析装置の管理下に存在する場合に、ルータレベル解析結果ホストが送出出したと断定されるパケットの情報を元にホスト内部解析を開始する(411、412)。その他の場合はホスト内部解析を開始しない(410)。このとき、同時に開始されたホストレベル解析によって既に別のホストに関するホスト内部解析プロセスが実行中であった場合(412)には、そのホスト内部解析プロセスを終了する(407)。ホスト内部解析終了時(405、406、408)、ホスト内部解析の入力としたパケットを生成したプロセスが、ネットワークを経由した外部装置からの命令を受信していた場合には、その命令を伝達したパケットを特定し、特定したパケットを入力とするホストレベル解析およびルータレベル解析を同時に起動する(405、406)。その他の場合はホストレベル解析、ルータレベル解析ともに開始しない(408)。これら全ての解析処理が終了した場合に侵入経路解析の終了とみなす(413)。

【0031】ここで、図4に示した例について概説する。ただし、便宜上、実行されるホストレベル解析、ルータレベル解析はいずれかのホストについてのホスト内部解析を可能であるという結果が得られるものとする。同様に、実行されるホスト内部解析結果は、407で終了された解析と408で終了する解析を除いて、ホスト内部解析の後に継続してホストレベル解析およびルータレベル解析を実行可能であるという結果が得られるものとする。ネットワークを流れるパケットを監視している侵入検知装置から侵入検知通知があり、401及び409においてホストレベル解析とルータレベル解析が同時に開始される。402においてホストレベル解析が完了し、ホストレベル解析の結果、侵入パケットの送信元として、侵入経路解析装置と同じネットワークに属するホストのいずれかが検出される。なお、以下では、侵入経路解析装置と同じネットワークに属するホストを内部ホストと記す。また、401～402のホストレベル解析で検出された内部ホストを内部ホストAと称する。40

2においてホストレベル解析が終了したときに、終了したホストレベル解析と同時に開始されたルータレベル解析が未終了である、引き続きホスト内部解析が行われる。ホスト内部解析では、ホストレベル解析で検出された内部ホストAの内部プロセスについて解析が行われる。一方、410においてルータレベル解析が完了するが、ルータレベル解析での検出結果は、先に完了しているホストレベル解析の検出結果と同じなので、ホスト内部解析はそのまま実行される。405で、ホスト内部解析が完了し、内部ホストAが受信したパケットのうち侵入パケットの生成及び送信に関与したパケット(以下、侵入パケットと記す)が特定される。405でホスト内部解析が完了したので、ホスト内部解析により特定された侵入パケットに対して、ホストレベル解析とルータレベル解析とが同時に開始される。411において、ルータレベル解析が完了し、ルータレベル解析の結果、侵入パケットの送信元として内部ホストBが検出される。ルータレベル解析により内部ホストBが検出されたので、内部ホストBの内部プロセス状況についてホスト内部解析が開始される。一方、403で、ホストレベル解析が完了するが、既にルータレベル解析の結果によるホスト内部解析が実行されているため、ルータレベル解析の結果を優先し、411で実行されたホスト内部解析を継続する。406で、ホスト内部解析が完了し、内部ホストBが受信したパケットのうち侵入パケットの生成及び送信に関与した侵入パケットが特定される。406でホスト内部解析が完了したので、ホスト内部解析により特定された侵入パケットに対して、ホストレベル解析とルータレベル解析とが同時に開始される。404で、ホストレベル解析が完了し、ホストレベル解析の結果、侵入パケットの送信元候補として内部ホストCが検出される。そして、ホストレベル解析で検出された内部ホストCの内部プロセス状況についてホスト内部解析が開始される。一方、412で、ルータレベル解析が完了し、ホストレベル解析で検出された内部ホストCと異なる内部ホストDが侵入パケットの送信元として検出される。この場合、ルータレベル解析での検出結果はホストレベル解析での検出結果よりも正確性が高いので、内部ホストCに対して実行中であったホスト内部解析を終了し、ルータレベル解析で検出された内部ホストDの内部プロセスについてホスト内部解析を開始する(407)。図4の例では、ホスト内部解析の結果、内部ホストの侵入パケット生成・侵入に関与したパケットが検出されなかつたので、内部ホストDを攻撃者の端末または攻撃者の端末が直結されたホストであると断定して全ての解析処理を終了する場合を示している(408、413)。

【0032】次に、ルータレベル解析の処理手順について説明する。まず、ルータレベル解析の基本的な原理について説明する。侵入経路解析装置は、侵入検知装置により、ホストへの侵入パケットが検知された場合に、検

知された侵入パケットのヘッダとデータ管理装置のデータベース内に格納されているヘッダ情報を比較し、Etherアドレス及びTTLを除き侵入パケットのヘッダと同じ内容のヘッダ情報を抽出する。この抽出されたヘッダ情報は、EtherアドレスとTTL以外の情報が侵入パケットのヘッダと一致しているので、侵入パケットに関するヘッダ情報であると考えることができる。そして、抽出されたヘッダ情報をについて送信元Etherアドレス、宛先Etherアドレス、TTLの更新経過を順次遡ることにより侵入パケットの送信元を検出する。以上が、ルータレベル解析の基本的な原理である。では、次に、図5、図6並びに、図7を参照しながら、ルータレベル解析について具体的に説明する。

【0033】図5において、501から505はホスト、506から508はルータ、509から512は各機器を結ぶネットワーク、513から516はパケット収集装置、517は侵入検知装置、M1からM11は各機器が持つEtherアドレスを表している。

【0034】図6において、601から613はそれぞれ図5のホスト501から504の計4つのホストからホスト505(Etherアドレス:M11)へパケットのヘッダが全く等しい(Etherアドレス及びTTLを除く)攻撃パケットを送信したとき、図5の侵入検知装置517が検知するパケット608、609、612、613の何れかを検索キーとしてデータベース検索を行って得られた検索結果を表す。ただし、図6では、得られた検索結果をヘッダ情報のTTL値によって分類して記載してある。ヘッダ情報は便宜上、発信元Etherアドレス、宛先Etherアドレス、TTL値と、それら以外の情報(パケットの検索に用いた、ICMPプロトコルヘッダのType、Code、Checksum、IPプロトコルヘッダのIdentification、Protocol、発信元IPアドレス、宛先IPアドレス、TCP/UDPプロトコルヘッダの発信元ポート番号、宛先ポート番号、Checksum、TCPプロトコルヘッダのSequenceNumber、AcknowledgmentNumberなどが含まれ、図6ではXで表記)の4つに区別して表される。図7において、701は図6のパケット609を検索キーとしてルータレベル解析を行った侵入経路解析結果、702は図6のパケット612(またはパケット613)を検索キーとしてルータレベル解析を行った侵入経路解析結果を表している。

【0035】ここでは、図6のパケット609のルータレベル解析を行うとする。パケット609を検索キーとしてデータベース検索を行った結果をIPプロトコルのTTL値によって分類すると図6のような分類が得られる。

【0036】次に、データベース検索により得られた結果に含まれるヘッダ情報のうち、パケット609のTT

L値より小さいTTL値を持つヘッダ情報を破棄する。これは、攻撃パケット送信ホストから攻撃を受けたホスト505までの経路上では、パケットの宛先IPアドレスが受信したパケットのTTL値が最小となることによる。したがって、TTL値として7を持つパケット612とパケット613は、ここでデータベース検索結果から破棄される。

【0037】TTL値がパケット609と同じ、8のものがデータベース検索により得られた結果に存在する場合には、TTL値が8に分類されるヘッダ情報から、パケット609と発信元Etherアドレス並びに、宛先Etherアドレスが等しいヘッダ情報以外のヘッダ情報を破棄する。したがって、パケット610とパケット611は、ここでデータベース検索結果から破棄される。

【0038】次にTTL値が9のヘッダ情報について処理を行う。まず、TTL値が8を持つパケットで残っているヘッダ情報（パケット609）の発信元Etherアドレスを持つルータ508が持つ全てのEtherアドレスを調べる。このとき、ルータ508はM10とM9をEtherアドレスとして持つことがわかる。次に、TTL値が9に分類されるヘッダ情報のうち、M10またはM9を宛先Etherアドレスとして持つパケット607を選択し、残りを破棄する。したがって、パケット605、パケット606、パケット608は、ここでデータベース検索結果から破棄される。

【0039】同様に、TTL値に9を持つパケットで残っているヘッダ情報（パケット607）の発信元EtherアドレスM8をEtherアドレスとして持つルータ507が持つ全てのEtherアドレスを調べる。このとき、ルータ507はM8とM7をEtherアドレスとして持つことがわかる。次に、TTL値が10に分類されるヘッダ情報のうち、M8またはM7を宛先Etherアドレスとして持つパケット603を選択し、残りを破棄する。したがって、パケット601、パケット602、パケット604は、ここでデータベース検索結果から破棄される。

【0040】TTL値に10を持つパケットで残っているヘッダ情報（パケット603）の発信元EtherアドレスM3をEtherアドレスとして持つルータが持つ全てのEtherアドレスを調べる。しかしながら、M3はルータが持つEtherアドレスではないため、M3をEtherアドレスとして持つルータは検出されない。ここで、パケット603は、EtherアドレスM3を持つホスト503から発信されたと断定する。したがって、パケット609は、ホスト503から発信されルータ507およびルータ508によって中継されホスト505へ到達したという、図7の701の結果が得られる。

【0041】図6のパケット612（もしくはパケット

613）に関して上記の処理を行った場合は、図5のホスト501とホスト502がともにパケットの発信ホストとして特定され、図7の702のような結果が得られる。

【0042】以上のように、ルータレベル解析は、パケットのIPアドレスによらず解析を行うので、IPアドレスを許された場合でも正確に侵入パケットの送出ホストと中継経路を特定できる反面、一般的には解析に時間がかかる。

【0043】ここでは、図8を参照しながら侵入パケットの情報を初期入力とするホスト内部解析の説明を行う。図8において、810はホスト（踏み台）、801から807はホスト810上で起動されたプロセス、811、812は外部装置、808は外部装置811との通信並びに、809は外部装置812との通信に使用されたホスト810上の通信ポートを表している。なお、外部装置とは、他のホストまたはルータを意味する。プロセス801からプロセス807の間には、他のプロセスによって起動された側と起動した側という、いわゆるプロセスの親子関係が成立している。たとえば、図8において、プロセス805、プロセス806は、プロセス804によって起動されている。この場合、プロセス805およびプロセス806をプロセス804の子プロセス、プロセス804をプロセス805、プロセス806親プロセスと呼ぶ。ここで、ホスト810は外部装置811から外部装置812へ攻撃を行う際の踏み台ホストとして使用されたものとする。

【0044】侵入経路を外部装置812の側から前述のホストレベル解析もしくは、ルータレベル解析が既に行われておらず、解析の結果、パケットはホスト810の通信ポート809から送信されたことが特定されているものとする。このとき、そのパケット取得日時を検索キーとしてデータベースを検索し、その時間にホスト810の通信ポート809を使用していたプロセス（パケット生成プロセス）に関する情報（プロセス生成日時、プロセス終了日時、プロセス識別子、親プロセス識別子、実ユーザ識別子、実行ユーザ識別子、実ダブルユーザ識別子、実行グループ識別子、実行ディレクトリ、実行コマンドバス、実行コマンドライン、通信開始日時、通信終了日時、通信先IPアドレス、通信先TCP/UDPポート番号、通信NICに割り当てられていたEtherアドレスとIPアドレス、TCP/UDPポート番号）を得る。このとき、パケット生成プロセスは外部装置からの接続による通信を確立していた場合（パケット受信プロセスが行われていた場合）は、通信開始日時、通信終了日時、通信先IPアドレス、通信先TCP/UDPポート番号、通信NICに割り当てられていたEtherアドレスとIPアドレス、TCP/UDPポート番号を検索キーとして、データベースを検索し、外部装置から受け取ったパケットを特定する。この特定したパケット

は、ホスト 810 の攻撃パケットの生成に関与したパケットである。そして、この特定したパケットについて、ルータレベル解析及びホストレベル解析を行い、このパケットの送信元を特定する。パケット生成プロセスが外部装置からの接続による通信を確立していなかった場合は、同様の処理を親プロセスに対して行う。

【0045】パケット生成プロセスが外部装置からの接続による通信を確立していたプロセスが見つかるか、親プロセスが定義されないプロセス（オペレーティングシステムの特別なプロセス）にたどり着くまで、上記の処理を繰り返し行う。親プロセスが定義されないプロセスにたどり着いた場合には、そのホストを、攻撃者が直接利用したコンピュータであると断定する。

【0046】図8の例では、プロセス 803 が外部装置からの接続による通信を確立していたプロセスとなるため、プロセス 803 に関する情報を検索キーとしてデータベースを検索し、プロセス 803 が外部装置から受け取ったパケットを特定する。

【0047】ホスト内部のプロセス情報を初期入力とするホスト内部解析（ホスト内部を監視する侵入検知装置により解析対象となるホストが特定された場合）では、上記のパケットの情報を初期入力とするホスト内部解析のホスト上でパケットを生成したプロセスに関する情報を得る処理から解析を開始し、後の処理は、パケットの情報を初期入力とする処理と同様である。

【0048】以上のように、ホストレベル解析、ルータレベル解析並びに、ホスト内部解析を行なって行うことから、解析結果の正確性を保証しつつ、高速に侵入経路解析を行うことができる。また、ヘッダ情報並びに、ホスト内部情報をデータ管理装置でデータベースにより集中管理するため、ホストレベル解析、ルータレベル解析並びに、ホスト内部解析を行なう際に、侵入経路解析中は各装置間で通信を行なながら、経路上の各ルータを逐次追跡する必要がないことからも侵入経路解析時間の短縮効果がある。

【0049】実施の形態2。以上の実施の形態1では、過去における侵入に関しても追跡可能するために、ネットワーク上を流れるパケットおよびホスト上のプロセスの情報を常時取得し、記録していた。この場合、記録したデータを保存するために、大容量の記憶領域を消費する。しかしながら、導入するシステムの環境によっては、データを保持しておくための大容量記憶領域の確保が難しい場合もあるため、以下のような方法により適宜情報を圧縮することもできる。第一に、記録する各パケットのデータのうち、侵入経路解析で用いる項目（パケット取得日時並びに、パケットを識別するために一般的に用いられるパケットヘッダ内の発信元 Ether アドレス、宛先 Ether アドレス、ICMP プロトコルヘッダの Type、Code、Checksum、IP プロトコルヘッダの Identification、TT

L、Protocol、発信元 IP アドレス、宛先 IP アドレス、TCP／UDP プロトコルヘッダの発信元ポート番号、宛先ポート番号、Checksum、TCP プロトコルヘッダの Sequence Number、Acknowledgment Number）だけを記録していく。第二に、侵入経路解析装置より侵入経路データ提出要求があったときのみ各パケット取得装置並びに、各ホスト内部情報収集装置で同時に情報収集を開始する。どちらの場合も、解析するシステムの大きさにより、データを保持する期間を決めて一定期間を過ぎたデータから随時削除していくことも可能である。

【0050】以上のように、常時保持するデータの量を制限することで、侵入経路解析に使用される記憶領域容量を軽減できる。ただし、データを保持しておく期間は、適用するシステムの性能並びに、要求される解析結果の詳細度によって決定される。

【0051】実施の形態3。以上の実施の形態1並びに実施の形態2では、少なくとも解析を行う段階においてデータベースに検索対象となるデータが格納されていれば侵入経路解析には影響を及ぼさない。したがって、各パケット取得装置並びに、各ホスト内部情報収集装置で収集したデータを常時データベース管理装置に格納する必要はなく、侵入経路解析を行わないときは、各パケット収集装置並びに、各ホスト内部情報収集装置で収集したデータを保持しておく、侵入経路解析を行う際に各装置から一齊に記録データ（パケットの情報並びに、ホスト上のプロセス情報）をデータ管理装置へ送信しデータベースへ格納することもできる。

【0052】以上の実施の形態3によれば、収集データの分散管理が可能であり、侵入経路解析未実行時のデータ管理装置上のリソースに対する負荷（記憶領域容量並びにデータ処理など）を削減できる。

【0053】実施の形態4。以上の実施の形態3では、侵入経路解析を行う際に各装置から一齊に記録データ（パケットの情報並びに、ホスト上のプロセス情報）をデータ管理装置へ送信しデータベースへ格納することで、侵入経路解析未実行時の収集データの分散管理を行なった。これに加え、各パケット収集装置上にルータレベル解析機能並びに、各ホスト内部情報収集装置上にホスト内部解析機能を備え、侵入経路解析装置が侵入経路解析のスケジューリング並びに、ホストレベル解析を行うように場合には、侵入経路解析時に侵入経路解析装置にかかる計算負荷を軽減できる。

【0054】以上の実施の形態4によれば、ネットワーク上に分散している各パケット収集装置並びに、各ホスト内部情報収集装置へ侵入経路解析処理を分散していくため、侵入経路解析時に侵入経路解析装置にかかる計算負荷を軽減できる。加えて、実装上パケット収集装置並びに、ホスト内部情報収集装置がそれぞれルータ並びにホスト上に実装されていた場合、当該不正アクセス処

理が継続中である場合には、ルータやホストのその他の処理を意図的に遅延されることも可能であり、不正アクセス処理を遅延する効果もある。

【0055】実施の形態5、以上の実施の形態1～4では、単一の侵入経路解析装置を用いた場合の実施の例であったため、侵入経路解析の範囲に限界がある。そこで、実施の形態5では、複数の侵入経路解析装置を用いて、より広範囲な侵入経路解析を行う方式について説明する。

【0056】図9において、901、902、903はそれぞれ異なる侵入経路解析装置、904、905、906はそれぞれ侵入経路解析装置901、902、903が経路解析可能なネットワーク、907～910は侵入経路上のホストを表している。なお、各ネットワークとも、図1に示したように、侵入検知装置、パケット収集装置等が配置されているものとする。各ホスト間を結ぶ直線上にはパケットを中継する複数のルータが存在している。図9では、ホスト907を攻撃者端末とし、攻撃者はホスト908およびホスト909を踏み台としてホスト910を攻撃したものとする。

【0057】侵入経路解析装置903は、前述の方法で侵入経路解析を行った結果、ホスト910への不正アクセスパケットは、侵入経路解析装置902によって追跡可能なネットワーク上の装置（ホストまたはルータ）から送信されたパケットであると断定する。このとき、侵入経路解析装置903は、ネットワーク905からネットワーク906へ送られてきたパケットの情報を含む検出依頼を侵入経路解析装置902に送信し、侵入経路解析の継続を依頼する。

【0058】検出依頼を受領した侵入経路解析装置902は、侵入経路解析装置903から送られてきたパケット情報を元に、実施の形態1～4に示す方式に従って侵入経路解析を行う。このとき、ネットワーク905上のホスト908およびホスト909が踏み台とされたこと、並びに、ホスト908は侵入経路解析装置901が解析可能なネットワーク上の装置（ホストまたはルータ）から送信されたパケットであると断定する。侵入経路解析結果を侵入経路解析装置903に送信する。

【0059】侵入経路解析装置903は、侵入経路解析装置902の解析結果に含まれる、侵入経路解析装置902からのパケット情報を含む検出依頼を侵入経路解析装置901へ送信し、侵入経路解析の継続を依頼する。

【0060】侵入経路解析装置901でも、侵入経路解析装置902と同様に侵入経路解析を行い、検出依頼のあったパケットは、ホスト907から発信されたことを特定し、解析結果を侵入経路解析装置903に送信する。

【0061】最終的に、侵入経路解析装置903は、ネットワーク906の解析結果、並びに、侵入経路解析装置902、侵入経路解析装置901から送信されてきた

結果から、ホスト907からホスト910までの一連の侵入経路を特定する。

【0062】以上の実施の形態5によれば、複数の侵入経路解析装置が連携し、個々のネットワーク内の解析結果を統合しているため、複数のネットワークにわたるような広範囲な侵入経路解析ができる。

【0063】以上の実施の形態1～5では、本発明に係る不正アクセス経路解析システム（侵入経路解析システム）について説明したが、実施の形態1～5に示した処理手順により本発明に係る不正アクセス経路解析方法も実現可能である。

【0064】ここで、実施の形態1～5に示した侵入経路解析システムの特徴を以下にて再言する。

【0065】実施の形態1～5に示す侵入経路解析システムは、以下の装置を有することを特徴とする。

1. 外部装置からの命令を受信もしくは、自動もしくは、手動で起動し、ネットワーク上を流れるパケットを収集し、記録し、外部装置による記録データ送信要求発行時もしくは、定期的に外部装置へ記録データを送信するパケット収集装置（複数可能）。

2. 外部装置からの命令を受信もしくは、自動もしくは、手動で起動し、オペレーティングシステムによって管理されるホスト上のプロセス管理情報並びに、そのプロセスのプロセス間通信履歴に関する情報（これらを総称してホスト内部情報と呼ぶことがある）を収集し、記録し、外部装置による記録データ送信要求発行時もしくは、定期的に外部装置へ記録データを送信するホスト内部情報収集装置（複数可能）。

3. ネットワーク上に存在するパケット収集装置並びに、ホスト内部情報収集装置へ記録データ送信要求発行時もしくは、定期的にパケット収集装置並びにホスト内部情報収集装置から送信される記録データを受信し、データベースに格納するデータ管理装置（複数可能）。

4. 外部装置からの命令を受信もしくは、自動もしくは、手動で起動し、ホストレベル解析機能、ルータレベル解析機能、ホスト内部解析機能を持ち、それぞれの解析を平行して実行可能である侵入経路解析装置（複数可能）。

5. ネットワーク上を流れるパケットを監視もしくはホストの内部状態を監視することで侵入を検知し、検知した情報を外部装置へ通知する侵入検知装置。

【0066】実施の形態1～5に示す侵入経路解析システムは、ヘッダ情報を検索キーとしてデータベース検索し、得られた複数の検索結果をパケット情報に含まれる TTL (Time to Live) データ、送信元Ethernetアドレス並びに、宛先Ethernetアドレスを用いて解析することを特徴とする。

【0067】実施の形態1～5に示す侵入経路解析システムは、ルータレベル解析と、ホスト内部情報を用いたホスト内部解析を行うことを特徴とする。

【0068】実施の形態1～5に示す侵入経路解析システムは、ルータレベル解析並びに、パケット情報に含まれる発信元IPアドレスによるパケットの発信元解析を行うホストレベル解析並びに、ホスト内部解析を併用して侵入経路解析を高速化することを特徴とする。

【0069】

【発明の効果】以上のように、本発明によれば、送信元検出処理及び内部プロセス解析処理を行うため、踏み台を介した不正アクセス、発信元アドレスを偽称した不正アクセスにも対応可能であり、解析結果の正確性を保証しつつ、高速に不正アクセス経路解析を行うことができる。

【0070】また、本発明によれば、第一の送信元検出処理と第二の送信元検出処理とを並行して行うため、第一の送信元検出処理により解析結果の正確性を保証することができ、また、第二の送信元検出処理により解析処理の高速化を図ることができる。

【0071】また、本発明によれば、パケットの収集及び内部プロセス情報の収集は、指示があった場合のみ行うため、ヘッダ情報及び内部プロセス情報の記憶のための記憶領域容量を軽減することができる。

【0072】また、本発明によれば、ヘッダ情報及び内部プロセス情報は、指示があった場合のみ送信することとしているため、不正アクセス経路解析を行わないときのシステムリソースに対する負荷を削減することができる。

【0073】また、本発明によれば、複数のネットワークに跨って不正アクセス経路解析を行うことができるた

め、広範囲に渡った不正アクセスの場合でも、正確かつ高速に不正アクセス経路解析を行うことができる。

【図面の簡単な説明】

【図1】 侵入経路解析システムのシステム構成例を示す図。

【図2】 従来の技術を説明する図。

【図3】 従来の技術を説明する図。

【図4】 侵入経路解析スケジューリング例を示す図。

【図5】 ルータレベル解析例を説明するためのシステム構成図。

【図6】 ヘッダ情報の例を示す図。

【図7】 ルータレベル解析の結果の例を示す図。

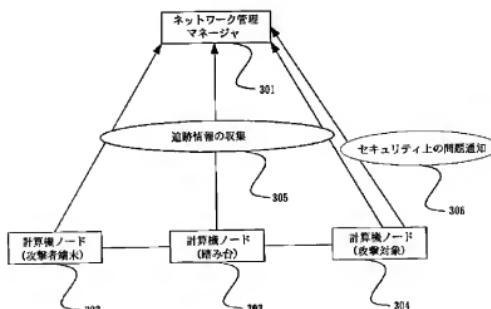
【図8】 ホスト内部解析例を説明するためのプロセス経過図。

【図9】 複数の侵入経路解析システムを用いた解析例を説明するためのシステム構成図。

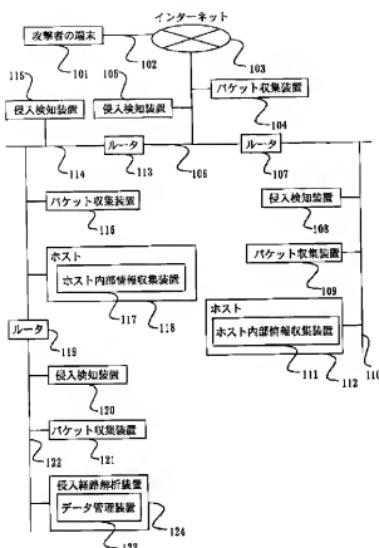
【符号の説明】

101 攻撃者の端末、102 経路、103 インターネット、104 パケット収集装置、105 侵入検知装置、106 サブネットワーク、107 ルータ、108 侵入検知装置、109 パケット収集装置、110 サブネットワーク、111 ホスト内部情報収集装置、112 ホスト、113 ルータ、114 サブネットワーク、115 侵入検知装置、116 パケット収集装置、117 ホスト内部情報収集装置、118 ホスト、119 ルータ、120 侵入検知装置、121 パケット収集装置、122 サブネットワーク、123 データ管理装置、124 侵入経路解析装置。

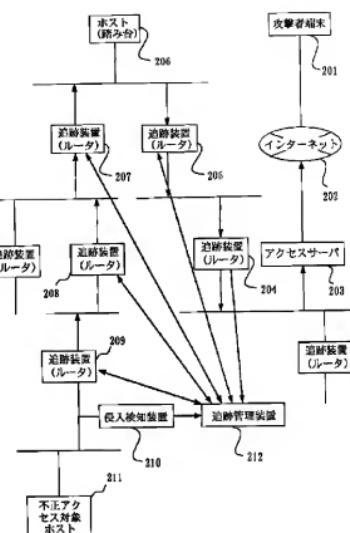
【図3】



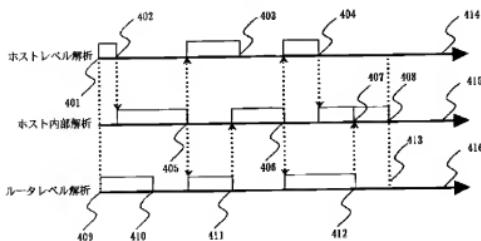
【图1】



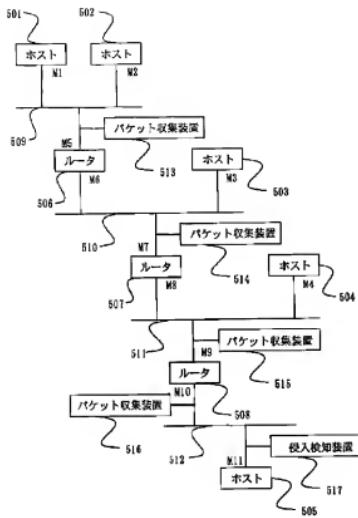
【图2】



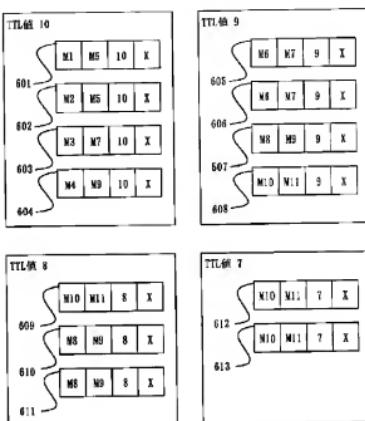
【图4】



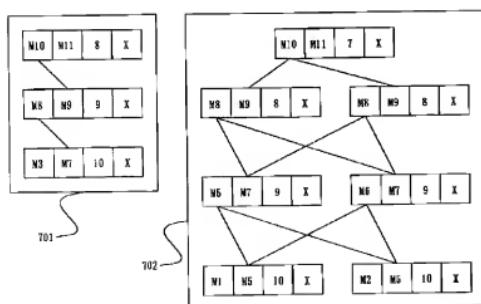
【図5】



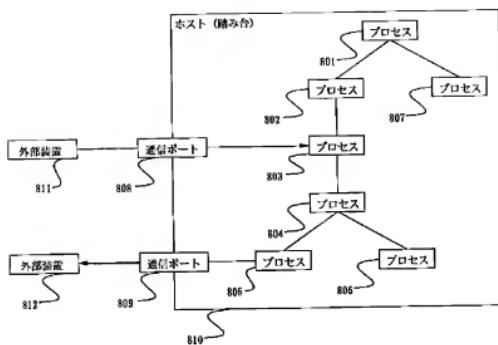
【図6】



【図7】



【図8】



【図9】

